Security Architecture Work Group

Monday January 27, 2003
10:30 A.M. to Noon
NSOB 6Y – Lincoln, NE

Minutes

A. Participants

Allan	Albers	HHSS
Mahendra	Bansal	Department of Natural Resources
Cathy	Danahy	Secretary of State / Records Management
Rick	Golden	University of Nebraska
Jerry	Hielen	IMServices
Kevin	Keller	IMServices
Joe	Kellner	Department of Roads
Leona	Roach	University of Nebraska
Linda	Salac	HHSS
Steve	Schafer	Nebraska CIO
Gary	Wieman	Legislative Council
Ron	Woerner	Department of Roads

B. Security Directory

Kevin Keller and Jerry Hielen gave a status report on the enterprise directory services project. IMServices is in the process of configuring the system and is looking for consensus on several issues pertaining to implementation. This includes things like classification levels, password reset policies, options for migrating from Guardian to the new directory, and the issue of determining a single identity for a person who is listed in several existing systems. Some agencies may not choose to use the enterprise directory for various reasons. IMServices will host four or five sessions to explain the options and get advice. If people want to attend the sessions, they should contact Kevin Keller.

C. Disaster Planning Next Steps

The NITC adopted the Disaster Recovery Planning Procedures at its November 2002 meeting. A copy is located at: http://www.nitc.state.ne.us/standards/index.html. Steve Schafer reported on efforts to link disaster planning for information technology to the broader subject of business continuity. The Nebraska Emergency Management Agency (NEMA) is updated the State Emergency Operations Plan, which includes a section on "Continuity of Government." The draft revisions include a new paragraph that discusses the need for continuity of operations. On January 16, Steve Schafer gave an overview on the state's overall readiness in this area to the Homeland Security Policy Group.

Discussion cited the need for high-level policy support and direction on several issues. In particular, what amount of preparedness should agencies plan for? What is the process for declaring an emergency and triggering interagency mutual aid? To be successful, there must be an effort to provide a joint infrastructure and shared solutions where necessary. To garner support, it may be necessary to conduct an assessment of the state's readiness to respond to a disaster that affects state government operations. A tabletop exercise and a third party review are two options for a readiness assessment.

Kansas is an example of a state that is taking an enterprise approach to disaster planning. The State of Kansas has a contract with SunGard to provide assistance to state agencies and local governmental units as they develop their business contingency plans. The Kansas web site (http://da.state.ks.us/disc/DR/default.htm) includes information on business continuity planning, a model plan, a template, and related links.

A volunteer approach to disaster planning will not work by itself. Someone must at least take on the role of focusing attention and coordinating among agencies and between Homeland Security and other issues.

D. Security Awareness

Jerry Hielen described their pilot project with the E-Moat web-based training. As part of a grant from the NITC, IMServices purchased more than a thousand temporary licenses. Less than a thousand people took the training. IMServices is now conducting a survey of those who used the product to evaluate whether it was worthwhile. DOR has purchased about 200 yearlong licenses for its IT staff. HHSS is looking at E-Moat or similar products to provide training on requirements stemming from HIPAA, human resources regulations, IRS regulations, and Social Security Administration regulations.

E. Remote Access Policy and Wireless Policy

Discussion reflected agreement on the need for guidelines pertaining to both remote access and the use of wireless networks. More agencies are allowing remote access to employees or business partners, and more agencies are implementing wireless capabilities. Texas and Iowa are two states that have developed good policies in these areas. Ron Woerner suggested that we use the NIST Computer Security Resource Center (http://csrc.nist.gov/publications/nistpubs/index.html), which has two documents that could be the basis for state guidelines:

- SP 800-48 Wireless Network Security: 802.11, Bluetooth, and Handheld Devices
- SP 800-46 Security for Telecommuting and Broadband Communications.

Prior to the next meeting, Steve Schafer will develop draft guidelines based on the NIST documents. He will look at others state's policies and the draft remote access standards under consideration at DOR.

F. Security Alerts

Participants expressed interest in being notified if a particular security threat is impacting other agencies. Early warning can sometimes help other agencies to take precautions and avoid problems. IMServices currently sends notices to a list of technical contacts. Discussion supported the following actions:

- People with security responsibilities should subscribe to resources such as one of the the NIPC services*;
- Agencies encountering security incidents should notify the IMServices Help Desk;
- If appropriate, IMServices Help Desk would broadcast information about the security problem to its list of technical contacts.
- The Security Work Group should consider whether to amend the Security Incident Reporting Procedures: http://www.nitc.state.ne.us/standards/index.html to reflect these steps.

G. Other Security Issues

The need for a policy on SPAM (unwanted bulk e-mail) was discussed. The State of Texas has adopted a policy with two sets of rules. One set governs when agencies can send out large numbers of e-mail messages. The other set addresses how to protect against SPAM. A copy of their standards is available at: http://www.dir.state.tx.us/standards/srrpub14.htm.

Ron Woerner reported that DOR is now using the Websense web filtering product (http://www.websense.com/). Websense maintains and keeps up to date an extensive list of websites with objectionable content. The software gives DOR flexibility to tailor a set of rules to meet their requirements.

Steve Schafer reported on the status of the external intrusion security assessment. Omni Tech Corporation won the bid. The project is slated to start on February 3 and last through the end of the June. It will consist of three phases – discovery, scanning, and testing. The first two phases pose little risk in terms of disruption of systems. The third phase will be conducted in close coordination with agencies. Steve will notify agencies about the security assessment. Because phase 3 will be on a subset of systems, agencies may request that they be excluded.

H. Next Meeting Dates

Monday February 24, 2003 at 10:30 A.M. NSOB 6Y
Monday March 31, 2003 at 10:30 A.M. NSOB 6Y

*NIPC Products &Contact Information

The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The NIPC provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the NIPC web-site (http://www.nipc.gov), one can quickly access any of the following NIPC products:

- NIPC Advisories - Advisories address significant threat or incident information that suggests a change in readiness posture, protective options and/or response.
- NIPC Alerts - Alerts address major threat or incident information addressing imminent or in-progress attacks targeting specific national networks or critical infrastructures.
- NIPC Information Bulletins - Information Bulletins communicate issues that pertain to the critical national infrastructure and are for informational purposes only.
- NIPC CyberNotes - CyberNotes is published to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.